UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

EX PARTE OLIVER ET AL.

U.S. PATENT APPLICATION NUMBER 10/776,677

FILING DATE: FEBRUARY 10, 2004

BRIEF ON APPEAL

LEWIS AND ROCA *LLP*
2440 W. EL CAMINO REAL, 6TH FLOOR
MOUNTAIN VIEW, CA 94040
T: 650.391.1386
F: 650.391.1395

ATTORNEY FOR THE APPELLANTS
AND REAL-PARTY-IN-INTEREST

TABLE OF CONTENTS

REAL-PARTY-IN-INTEREST
(37 C.F.R. § 41.37(c)(1)(i))

The Appellants in the present appeal are Jonathan Oliver and David A. Koblas—the inventors of U.S. patent application 10/776,677 (the '677 application). The real-party-in-interest is SonicWALL, Inc. by virtue of assignment from the inventors.

RELATED APPEALS AND INTERFERENCES
(37 C.F.R. § 41.37(c)(1)(ii))

U.S. patent application numbers 11/927,477 (the '477 application) and 12/070,164 (the '164 application) claim the priority benefit of the '677 application. A notice of appeal was filed with respect to the '477 application on May 11, 2011. The '164 application is currently on appeal before the Board of Appeals and Interferences and has been assigned appeal number 2001-005025.

STATUS OF THE CLAIMS
(37 C.F.R. § 41.37(c)(1)(iii))

Claims 1, 3-11, 13-17, 19-21, 23-35 are all pending and under appeal. All of the aforementioned claims have been at least twice rejected. Claims 2, 12, 18, 22, and 36 have been cancelled. No claims have been allowed or are otherwise objected to by the Examiner.

STATUS OF AMENDMENTS
(37 C.F.R. § 41.37(c)(1)(iv))

The amendments filed by Appellants on November 17, 2010 were acknowledged in the final office action dated December 1, 2010. No further amendments were filed by Appellants before filing the notice of appeal on May 2, 2011.

SUMMARY OF THE CLAIMED SUBJECT MATTER
(37 C.F.R. § 41.37(c)(1)(v))[1]

Independent claim 1 as presented for appeal recites:

> 1. A method of classifying a message transmitted over a network, the method comprising:
>
> maintaining a reputation table in memory, the reputation table including information regarding a plurality of address-domain pairs, each of the plurality of address-domain pairs indicating an IP address and an associated domain of a previously received message, the information regarding each of the plurality of address-domain pairs including one or more classification variables, the one or more classification variables decaying with time;
>
> receiving the message transmitted over the network;
>
> executing instructions stored in a non-transitory computer-readable storage medium to:
>
> determine an associated domain from which the received message is purported to be sent,
>
> identify that the determined domain appears on a whitelist,
>
> determine an IP address corresponding to a device from which the received message was relayed,
>
> associate the determined domain with the IP address to create an address-domain pair for the received message;
>
> classify the received message based on a score assigned to the address-domain pair, the score comprising a ratio of a first classification variable of the address-domain pair to a second classification variable of the address-domain pair as indicated by the reputation table, and
>
> override the whitelist based on the score assigned to the address-domain pair, wherein the received message is classified as spam even though the domain of the received message appears on the whitelist.

"The reputation table includes information about previous classifications made to various IP address and domain pairs." *Specification*, 11:14-15. "[A] reputation table can

---

[1] All references to the *SPECIFICATION* are exemplary and are not intended to be limiting. The present references are made solely to satisfy the requirements of 37 C.F.R. § 41.37(c)(1)(v). No reference is intended—nor should it be construed—as an admission or denial as to any requirement for patentability, including but not limited to those requirements set forth in 35 U.S.C. § 112, ¶ 1 as they pertain to written description and enablement.

be constructed and maintained to reflect previous classifications of received messages." *Specification*, 13:5-7. "In some embodiments, information is stored in the form of classification variables." *Specification*, 11:19-20. "In some embodiments, the classification variables are decayed over time to reduce the effects of older classifications." *Specification*, 13:13-14.

"It is difficult for a spammer to send a spam message with a forged sender domain of "anycompany.com" which also forges the boundary IP address. Therefore, if anycompany.com is whitelisted, it is very likely that messages purporting to be from anycompany.com originating from the IP addresses that have become associated with anycompany.com should enjoy automatic acceptance as a result of the whitelist. ." *Specification*, 6:19-7:2.

""An incoming message can be classified based on one or more IP addresses and a domain (or domain name) associated with the message." *Specification*, 4:20-21. "In some embodiments, the score is a ratio of spam classifications to good classifications." *Specification*, 14:2-3.

"Classifying may include any determination of the nature of a message including determining that it is likely to be spoofed or determining that it is appropriate to override a white list or a black list that controls the disposition of such a message." *Specification*, 5:18-20. "A white list can be overridden if the IP address and domain based classification provides compelling evidence that the message was not really sent from the stated sender domain." *Specification*, 7:14-16.

Independent claim 35 as presented for appeal recites:

> 35. A non-transitory computer-readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for classifying a message transmitted over a network, the method comprising:
>
> determining an associated domain from which a received message is purported to be sent,
>
> identifying that the determined domain appears on a whitelist,
>
> determining an IP address from which the received message was relayed,
>
> associating the determined domain with the IP address to create an address-domain pair for the received message;
>
> classifying the received message based on a score assigned to the address-domain pair, the score comprising a ratio of a first classification variable of the address-domain pair to a second classification variable of the address-domain pair, the first classification variable and the second classification variable indicated by a reputation table including information regarding a plurality of address-domain pairs, each of the plurality of address-domain pairs indicating an IP address and an associated domain of a previously received message, the information regarding each of the plurality of address-domain pairs including one or more classification variables, the one or more classification variables decaying with time, and
>
> override the whitelist based on the score assigned to the address-domain pair, wherein the received message is classified as spam even though the domain of the received message appears on the whitelist.

"The invention can be implemented in numerous ways, including as a process, an apparatus, a system, a composition of matter, a computer readable medium such as a computer readable storage medium or a computer network wherein program instructions are sent over optical or electronic communication links." *Specification*, 4:2-5. "The reputation table includes information about previous classifications made to various IP address and domain pairs." *Specification*, 11:14-15. "[A] reputation table can be constructed and maintained to reflect previous classifications of received messages." *Specification*, 13:5-7. "In some embodiments, information is stored in the form of classification variables." *Specification*, 11:19-20. "In some embodiments, the

classification variables are decayed over time to reduce the effects of older classifications." *Specification*, 13:13-14.

"It is difficult for a spammer to send a spam message with a forged sender domain of "anycompany.com" which also forges the boundary IP address. Therefore, if anycompany.com is whitelisted, it is very likely that messages purporting to be from anycompany.com originating from the IP addresses that have become associated with anycompany.com should enjoy automatic acceptance as a result of the whitelist. ." *Specification*, 6:19-7:2.

""An incoming message can be classified based on one or more IP addresses and a domain (or domain name) associated with the message." *Specification*, 4:20-21. "In some embodiments, the score is a ratio of spam classifications to good classifications." *Specification*, 14:2-3.

"Classifying may include any determination of the nature of a message including determining that it is likely to be spoofed or determining that it is appropriate to override a white list or a black list that controls the disposition of such a message." *Specification*, 5:18-20. "A white list can be overridden if the IP address and domain based classification provides compelling evidence that the message was not really sent from the stated sender domain." *Specification*, 7:14-16.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
(37 C.F.R. § 41.37(C)(1)(vi))

I. Has the Examiner Evidenced a *Prima Facie* Case of Obviousness under 35 U.S.C. § 103 with Respect to *Kirsch* and *Wang*?

ARGUMENT
(37 C.F.R. § 41.37(c)(1)(vii))

I. THE EXAMINER HAS NOT EVIDENCED A *PRIMA FACIE* CASE OF OBVIOUSNESS WITH RESPECT TO *KIRSCH* AND *WANG*

The Examiner maintains rejections of independent claims 1 and 35 as obvious based on U.S. patent number 7,206,814 (hereinafter *Kirsch*) in view of U.S. patent application number 2008/0040439 (hereinafter *Wang*). *December 1, 2010 Office Action*, 4. The Examiner further rejects claims 4 and 32 as obvious based on *Kirsch* and *Wang* in view of U.S. patent application number 2004/0068542 (hereinafter *Lalonde*). *December 1, 2010 Office Action*, 10. In addition, claims 6, 11, 20, 21, and 23-27 are rejected as obvious based on *Kirsch* and *Wang* in view of U.S. patent number 7,366,761 (hereinafter *Murray*). *December 1, 2010 Office Action*, 11. In addition, claim 29 is rejected as obvious based on *Kirsch* and *Wang* in further view of U. S. patent application number 2005/0076240 (hereinafter *Appleman*). *December 1, 2010 Office Action*, 13 The Appellants respectfully traverse.

A. Kirsch and *Wang*– *Individually, Collectively, or in Any Combination with Lalonde, Murray or Appleman- Fail to Disclose All Claim Limitations*

To support a conclusion that the claim would have been obvious requires that **all** the claimed elements were known in the prior art and that one skilled in the art could have combined those elements. See *KSR v. Teleflex*, 127 S.Ct. 1727, 1739 (2007); see also MPEP § 2143. The Appellants submit that *Kirsch* and *Wang*– individually or in any combination with *Lalonde*, *Murray*, or *Appleman* -- fail to disclose all the elements of the independent claims, including 'overrid[ing] the whitelist based on the score assigned to the address-domain pair, wherein the message is **classified as spam even though the domain of the message appears on the whitelist**.' Support can be found in the specification. See *e.g.*, *Specification*, 7:14-16; 16:8-9 (describing that "[a] white list can be overridden if the IP address and domain based classification provides compelling

evidence that the message was not really sent from the stated sender domain" and a "message may be classified as spam even if the user has that domain white listed, because of the strong evidence that that IP address is not a legitimate one").

The Examiner has already admitted that "*Lalonde*, *Kirsch*, and *Wang* **do not teach overriding a whitelist**." *March 26, 2010 Office Action*, 7. Notwithstanding, the Examiner attempts to argue that *Kirsch* teaches the claimed 'overrid[ing] the whitelist.' December 1, 2010 *Office Action*, 3. Specifically, the Examiner references "col. 19, lines 7-14' of *Kirsch*, which is reproduced below as follows:

> In other embodiments, the Inbox as well as the spam folder is also periodically evaluated to determine if the rating of any of the senders of messages in the Inbox has changed. If the sender's reputation is no longer "good," and the sender **has not been explicitly whitelisted** by the recipient, the message can be removed to a spam folder and processed accordingly or deleted, depending on the rating an the recipient's settings.

Kirsch, 19:7-14 (emphasis added). The Examiner claims that the section of *Kirsch* provided above "teach message of sender in the whitelist (message in the Inbox) can be changed to spam based on the calculated reputation of the sender from IP address and domain pair" and "[t]his means changing to spam counteracts the normal operation of the whitelist." *December 1, 2010 Office Action*, 14. As can be seen, however, *Kirsch* cannot teach the claimed override of the whitelist, but it notes that the sender has **not** been whitelisted. As such, there can be no whitelist to override, and the action described cannot teach the claimed whitelist override. *Kirsch* therefore fails to teach the claimed 'overrid[ing] the whitelist based on the score assigned to the address-domain pair, wherein the message is classified as spam even though the domain of the message appears on the whitelist.'

Kirsch states that "if the sender is on the whitelist, the message is passed on to the recipient." *Kirsch*, 60-61.

Moreover, *Kirsch* describes its whitelist as follows:

> [T]he message is added to the whitelist. Therefore, assuming that the user does not subsequently remove the message from the whitelist, future messages from the same sender to the same recipient **will be** passed to the recipient because the sender is on the whitelist.

Kirsch, 14:21-26 (emphasis added). *Kirsch* explicitly notes that when a message is added to a whitelist, it "will be" passed to the recipient. The exception is where the message is explicitly removed from the whitelist by the user. Once the message is removed from the whitelist, however, there is no longer any whitelist that can be overridden with respect to that message.

Wang, *Lalonde*, *Murray*, and *Appleman* do not overcome the deficiencies of *Kirsch* in this regard. In light of the foregoing, the Appellants contend that *Kirsch*, *Wang*, *Lalonde*, *Murray*, and *Appleman* -- individually or in any combination -- fail to teach all the limitations of the independent claims. Further, as each dependent claim incorporates each and every element of the claim upon which it depends, the dependent claims are allowable for at least the same reasons.

CONCLUSION AND REQUESTED RELIEF

Kirsch and *Wang*– individually or in any combination with *Lalonde*, *Murray*, or *Appleman* -- fail to teach each and every claim limitation of the independent claims, including at least the claimed 'overrid[ing] the whitelist based on the score assigned to the address-domain pair, wherein the message is **classified as spam even though the domain of the message appears on the whitelist**.'

Any claim dependent upon the aforementioned independent claims —either directly or via an intermediate dependent claim—is allowable for at least the same reasons as the independent claim from which it depends. As such, each and every one of the dependent claims of the present application are also in condition for allowance. For at least these reasons, the Examiner's rejection should be withdrawn.

Respectfully submitted,
Jonathan Oliver et al.

September 6, 2011

By: /Tam Thanh Pham/

Tam Thanh Pham (Reg. No. 50,565)
LEWIS AND ROCA *LLP*
2440 W. El Camino Real, 6th Floor
Mountain View, CA 94040
T: 650.391.1386
F: 650.391.1395

ATTORNEY FOR THE APPELLANTS
AND REAL-PARTY-IN-INTEREST

CLAIMS APPENDIX
(37 C.F.R. § 41.37(c)(1)(viii))

1. A method of classifying a message transmitted over a network, the method comprising:

maintaining a reputation table in memory, the reputation table including information regarding a plurality of address-domain pairs, each of the plurality of address-domain pairs indicating an IP address and an associated domain of a previously received message, the information regarding each of the plurality of address-domain pairs including one or more classification variables, the one or more classification variables decaying with time;

receiving the message transmitted over the network; and

executing instructions stored in a non-transitory computer readable storage medium to:

determine an associated domain from which the received message is purported to be sent,

identify that the determined domain appears on a whitelist,

determine an IP address corresponding to a device from which the received message was relayed,

associate the determined domain with the IP address to create an address-domain pair for the received message;

classify the received message based on a score assigned to the address-domain pair, the score comprising a ratio of a first classification variable of the address-domain pair to a second classification variable of the address-domain pair as indicated by the reputation table, and

override the whitelist based on the score assigned to the address-domain pair, wherein the received message is classified as spam even though the domain of the received message appears on the whitelist.

3. The method of claim 1, wherein classifying the received message is further based on classification variables associated with another address-domain pair, the other address-domain pair having a related IP address or related domain.

4. The method of claim 1, wherein classifying the received message is further based on classifications of other messages associated with the domain of the received message, the other messages further being associated with IP addresses other than the IP address of the received message.

5. The method of claim 1, wherein a plurality of IP addresses is associated with the domain.

6. The method of claim 1, wherein the IP address is associated with a plurality of domains.

7. The method of claim 1, wherein the IP address is a boundary IP address.

8. The method of claim 1, wherein the IP address is preconfigured.

9. The method of claim 1, wherein the IP address is preconfigured to be one hop from a gateway IP address.

10. The method of claim 1, wherein the IP address is learned.

11. The method of claim 1, wherein the IP address is adaptively determined.

13. The method of claim 10, wherein the IP address is a boundary IP address and wherein the boundary IP address is learned by detecting a pattern in a certain number of previously received messages.

14. The method of claim 1, wherein determining the domain from which the received message is purported to be sent includes identifying the stated sender domain associated with the received message.

15. The method of claim 1, wherein the domain is a domain associated with a boundary IP address.

16. The method of claim 1, wherein classifying the received message is further based on consulting a white list.

17. The method of claim 1, wherein classifying the received message is further based on previous classifications made to the address-domain pair.

19. The method of claim 1, wherein assigning the score includes determining a spam ratio.

20. The method of claim 1, wherein assigning the score includes determining a spam rate.

21. The method of claim 1, wherein assigning the score includes determining an estimated instantaneous spam rate.

23. The method of claim 1, wherein classifying the received message includes giving a classification variable greater weight relative to another classification variable.

24. The method of claim 1, wherein classifying the received message includes giving a classification variable associated with user classification greater weight relative to a classification variable associated with computer classification.

25. The method of claim 1, wherein classifying the received message includes giving an indeterminate classification a fraction of the weight of a good classification.

26. The method of claim 1, wherein the reputation table is indexed by IP address and domain.

27. The method of claim 1, wherein each cell of the reputation table includes information about previous classifications.

28. The method of claim 1, further comprising providing the classification of the received message based on the address-domain pair as input to another classifier.

29. The method of claim 28, wherein the other classifier is a Bayesian classifier.

30. The method of claim 1, wherein classifying the received message is further based on a score assigned to the IP address.

31. The method of claim 1, wherein classifying the received message is further based on a score assigned to the domain.

32. The method of claim 1, further comprising determining that the received message was forged based on the score assigned to the domain.

33. The method of claim 30, further comprising determining the score assigned to the IP address.

34. The method of claim 31, further comprising determining the score assigned to the domain.

35. A non-transitory computer-readable storage medium having embodied thereon a program, the program being executable by a processor to perform a method for classifying a message transmitted over a network, the method comprising:

determining an associated domain from which a received message is purported to be sent;

identifying that the determined domain appears on a whitelist,

determining an IP address from which the received message was relayed;

associating the determined domain with the IP address to create an address-domain pair for the received message;

classifying the received message based on a score assigned to the address-domain pair, the score comprising a ratio of a first classification variable of the address-domain pair to a second classification variable of the address-domain pair, the first classification variable and the second classification variable indicated by a reputation table including information regarding a plurality of address-domain pairs, each of the plurality of address-domain pairs indicating an IP address and an associated domain of a previously received message, the information regarding each of the plurality of address-domain pairs including one or more classification variables, the one or more classification variables decaying with time, and

overriding the whitelist based on the score assigned to the address-domain pair, wherein the received message is classified as spam even though the domain of the received message appears on the whitelist.

EVIDENCE APPENDIX
37 C.F.R. § 41.37(c)(1)(ix)

Not applicable in the present appeal.

RELATED PROCEEDINGS APPENDIX
37 C.F.R. § 41.37(c)(1)(x)

- Appeal Brief from U.S. patent application number 12/070,164
- Reply Brief from U.S. patent application number 12/070,164